

I hereby certify that this correspondence is being deposited with the United States Postal Service, with sufficient postage, as first class mail in an envelope addressed to:  
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

on June 18, 2004

Date of Deposit

Tadashi Horie Reg. No. 40,437

Name of applicant, assignee or  
Registered Representative

*Tadashi Horie*

Signature

June 18, 2004

Date of Signature

Case No. 9683/177

### IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Masayuki TSUDA et al.

Serial No.: 10/810,503

Filing Date: March 26, 2004

For: TERMINAL DEVICE AND PROGRAM

Examiner: To Be Assigned

Group Art Unit No.: 2122

### SUBMISSION OF CERTIFIED COPY OF FOREIGN PRIORITY DOCUMENT

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

Applicants submit herewith a certified copy of Japanese Patent Application No. 2003-091294 filed March 28, 2003, to which the above-identified United States Patent Application claims the right of foreign priority under 35 U.S.C. § 119.

Respectfully submitted,

*Tadashi Horie*

Tadashi Horie

Registration No. 40,437

Attorney for Applicant(s)

BRINKS HOFER GILSON & LIONE  
P.O. BOX 10395  
CHICAGO, ILLINOIS 60610  
(312) 321-4200

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 3 年    3 月 2 8 日  
Date of Application:

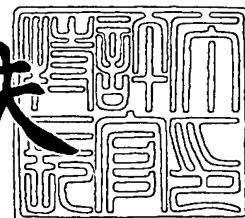
出 願 番 号                      特 願 2 0 0 3 - 0 9 1 2 9 4  
Application Number:  
[ST. 10/C]:                      [ J P 2 0 0 3 - 0 9 1 2 9 4 ]

出      願      人                      株式会社エヌ・ティ・ティ・ドコモ  
Applicant(s):

2 0 0 4 年    3 月 2 6 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号    出証特 2 0 0 4 - 3 0 2 5 4 7 8

【書類名】 特許願

【整理番号】 DCMH140781

【提出日】 平成15年 3月28日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 9/00  
H04Q 7/28

【発明の名称】 端末装置およびプログラム

【請求項の数】 5

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 津田 雅之

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 富岡 淳樹

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 渡邊 信之

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 服部 易憲

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 成瀬 直樹

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 市川 裕一

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 西田 真和

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 浅井 真生

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 大井 達郎

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 竹下 理人

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 山田 和宏

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 神谷 大

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ ・ ティ ・ ドコモ内

【氏名】 鷲尾 諭

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ ・ ティ ・ ドコモ内

【氏名】 山根 直樹

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ ・ ティ ・ ドコモ内

【氏名】 村上 圭一

## 【特許出願人】

【識別番号】 392026693

【氏名又は名称】 株式会社エヌ ・ ティ ・ ティ ・ ドコモ

## 【代理人】

【識別番号】 100098084

【弁理士】

【氏名又は名称】 川▲崎▼ 研二

## 【選任した代理人】

【識別番号】 100111763

【弁理士】

【氏名又は名称】 松本 隆

## 【手数料の表示】

【予納台帳番号】 038265

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1  
【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 端末装置およびプログラム

【特許請求の範囲】

【請求項 1】 データを記憶する第 1 の記憶手段と、  
アプリケーションプログラムに従って命令コードを実行する実行手段と、  
前記実行手段により実行可能な命令コードのうち、本端末装置において実行を制限されている命令コードを特定するデータを記憶する第 2 の記憶手段と、  
前記アプリケーションプログラムに従って前記実行手段により実行される命令コードが実行を制限されている命令コードであるか否かを前記第 2 の記憶手段の記憶内容に基づいて判定する判定手段と、  
実行を制限されている命令コードであると前記判定手段により判定され、かつ、該命令コードを実行することにより前記データの少なくとも一部分がアクセスされる場合には、該命令コードを前記実行手段が実行することを禁止する禁止手段と

を有する端末装置。

【請求項 2】 前記判定手段は、前記実行手段により実行されるアプリケーションプログラムがユーザにとって不利益な動作を行わないことが確認されていないアプリケーションプログラムである場合にのみ、該アプリケーションプログラムに従って実行される命令コードが実行を制限されている命令コードであるか否かを前記第 2 の記憶手段の記憶内容に基づいて判定する

ことを特徴とする請求項 1 に記載の端末装置。

【請求項 3】 通信網を介して通信する通信手段を備え、  
前記判定手段は、前記実行手段により実行されるアプリケーションプログラムが前記通信手段により前記通信網を介して取得されたアプリケーションプログラムである場合にのみ、該アプリケーションプログラムに従って実行される命令コードが実行を制限されている命令コードであるか否かを前記第 2 の記憶手段の記憶内容に基づいて判定する

ことを特徴とする請求項 1 に記載の端末装置。

【請求項 4】 前記第 1 の記憶手段は、データに該データのセキュリティを

保護するか否かを示す識別子を対応付けて記憶し、

前記禁止手段は、前記判定手段より実行を制限されている命令コードであると判定され、かつ、該命令コードにより前記第1の記憶手段にセキュリティを保護する旨の識別子を対応付けて記憶されている前記データの少なくとも一部分がアクセスされる場合には、該命令コードを前記実行手段が実行することを禁止することを特徴とする請求項1に記載の端末装置。

【請求項5】 データを記憶するとともに、自装置において実行を制限されている命令コードを特定するデータを記憶したコンピュータ装置に、

アプリケーションプログラムに従って命令コードを実行する実行手段と、

前記アプリケーションプログラムに従って前記実行手段により実行される命令コードが実行を制限されている命令コードであるか否かを該コンピュータ装置の記憶内容に基づいて判定する判定手段と、

実行を制限されている命令コードであると前記判定手段により判定され、かつ、該命令コードを実行することにより前記データの少なくとも一部分がアクセスされる場合には、該命令コードを前記実行手段が実行することを禁止する禁止手段と

を実現させるためのプログラム。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

端末装置に記憶されているデータのセキュリティを確保し、ユーザのプライバシーを保護する技術に関する。

##### 【0002】

#### 【従来の技術】

プログラム実行機能を有する携帯電話機やパーソナルコンピュータ装置（以下、「PC」という）などの端末装置が普及している。ユーザは、この種の端末装置にアプリケーションプログラムを実行させることにより、ゲームやスケジューラなどの様々なアプリケーションを利用することができる。このようなアプリケーションプログラムには、端末装置の販売以前にその不揮発性記憶部に書き込ま



れて提供されるものと、アプリケーションプログラム単独で提供され、端末装置の販売後にユーザによりインストールされるものとがある。以下では、前者を「ネイティブアプリケーションプログラム」と称し、後者を「非ネイティブアプリケーションプログラム」と称する。非ネイティブアプリケーションプログラムの一例としては、インターネットを介して提供されるアプリケーションプログラムや、C D - R O M (Compact Disk-Read Only Memory) のようなコンピュータ装置読み取り可能な記録媒体に記録されて提供されるアプリケーションプログラムが挙げられる。ユーザは各自のニーズに応じた非ネイティブアプリケーションプログラムをインストールすることにより、端末装置の機能を自由に追加および変更することができる。

#### 【 0 0 0 3 】

一般にアプリケーションプログラムは、ユーザのニーズに応じた機能を端末装置に実現させるためのものであるから、ユーザにとって有益なものである。しかしながら、アプリケーションプログラムの提供者（コンテンツプロバイダ；以下、「C P」と称する）に悪意がある場合には、そのアプリケーションプログラムを実行することでユーザが予期せぬ不利益を被ってしまう虞がある。具体的には、端末装置に記憶されている重要なデータ（例えば、ユーザの個人情報）がアプリケーションプログラムの実行過程で勝手に読み出され、C Pへ送信されてしまうような事態が生じ得る。ネイティブアプリケーションプログラムについては、例えば、端末装置の製品出荷時点での製品検査により、そのような事態が生じないことが端末装置の製造者によって確認されている。一方、非ネイティブアプリケーションプログラムについては、必ずしも、そのような確認が為されているわけではない。つまり、非ネイティブアプリケーションプログラムについては、そのアプリケーションプログラムを実行することで、ユーザが予期せぬ不利益を被ることがないとは言い切れない。

#### 【 0 0 0 4 】

ユーザが予期せぬ不利益を被らないようにするために、非ネイティブアプリケーションプログラムの利用を禁止し、ネイティブアプリケーションプログラムのみを利用させることが考えられる。しかし、非ネイティブアプリケーションプロ

グラムの利用を禁止されてしまうと、ユーザは各自のニーズに応じて端末装置の機能を自由に追加することや変更することができず、甚だ不便である。そこで、非ネイティブアプリケーションプログラムの利用を可能にしつつ、その非ネイティブアプリケーションプログラムの実行過程でユーザが予期せぬ不利益を被らないようにするための技術として特許文献 1 に開示されている技術がある。

#### 【0005】

特許文献 1 に開示されている技術では、データとそのデータを処理するためのプログラムとを論理的に一体化したオブジェクトを提供することにより、プログラムの提供が行われる。そして、このようなプログラムの利用を所望するユーザは、このプログラムを内包しているオブジェクトと、このプログラムを実行する際に必要となるリソース（メモリなどのハードウェア資源や、メモリに格納されているデータなどのソフトウェア資源）を取り決めるための契約を結び、この契約により定められリソースのみを利用させる。このようにして、プログラムに利用させるリソースを予め制限することにより、そのプログラムの実行過程で他のリソースが利用されることを禁止し、他のリソースについてのセキュリティを確保している。以下では、オブジェクトに内包されているデータを処理するために、そのデータとともに一体化されたプログラムを「メソッド」と称する。

#### 【0006】

##### 【特許文献 1】

特開 2002-245012 号公報

#### 【0007】

##### 【発明が解決しようとする課題】

上述したように、特許文献 1 に開示されている技術によれば、非ネイティブアプリケーションプログラムの実行過程で端末装置 10 に記憶されている重要なデータへアクセスすることを禁止する旨の契約を結んだ上で、この非ネイティブアプリケーションプログラムを実行し、この重要なデータのセキュリティを確保することができる。

#### 【0008】

しかしながら、非ネイティブアプリケーションプログラムの実行過程で利用可

能なリソースが制限されてしまうと、非ネイティブアプリケーションプログラムを設計する際の設計自由度が狭められてしまう。このように設計自由度が狭められてしまうと、その非ネイティブアプリケーションプログラムを実行することにより実現される機能も自ずから制限されてしまう。このような機能制限が伴う非ネイティブアプリケーションプログラムでは、ユーザの多用なニーズにきめ細やかに対応することはできないといった問題点がある。

#### 【 0 0 0 9 】

本発明は上記問題に鑑みて為されたものであり、端末装置に記憶されている重要なデータを非ネイティブアプリケーションプログラムが利用することを可能にしつつ、この重要なデータのセキュリティを確保する技術を提供することを目的としている。

#### 【 0 0 1 0 】

##### 【課題を解決するための手段】

上記課題を解決するため、本発明は、データを記憶する第 1 の記憶手段と、アプリケーションプログラムに従って命令コードを実行する実行手段と、前記実行手段により実行可能な命令コードのうち、本端末装置において実行を制限されている命令コードを特定するデータを記憶する第 2 の記憶手段と、前記アプリケーションプログラムに従って前記実行手段により実行される命令コードが実行を制限されている命令コードであるか否かを前記第 2 の記憶手段の記憶内容に基づいて判定する判定手段と、実行を制限されている命令コードであると前記判定手段により判定され、かつ、該命令コードを実行することにより前記データの少なくとも一部分がアクセスされる場合には、該命令コードを前記実行手段が実行することを禁止する禁止手段とを有する端末装置を提供する。

#### 【 0 0 1 1 】

このような端末装置によれば、アプリケーションプログラムに従って実行される命令コードのうち、実行を制限されている命令コードについては、その命令コードを実行することにより該端末装置に記憶されているデータが操作される場合には、その命令コードは実行されない。

#### 【 0 0 1 2 】

また、上記課題を解決するために、本発明は、データを記憶するとともに、自装置において実行を制限されている命令コードを特定するデータを記憶したコンピュータ装置に、アプリケーションプログラムに従って命令コードを実行する実行手段と、前記アプリケーションプログラムに従って前記実行手段により実行される命令コードが実行を制限されている命令コードであるか否かを該コンピュータ装置の記憶内容に基づいて判定する判定手段と、実行を制限されている命令コードであると前記判定手段により判定され、かつ、該命令コードを実行することにより前記データの少なくとも一部分がアクセスされる場合には、該命令コードを前記実行手段が実行することを禁止する禁止手段とを実現させるためのプログラムを提供する。

### 【0013】

このようなプログラムによれば、係るプログラムに従って作動するとともに、データと自装置で実行を制限されている命令コードを特定する識別子とを記憶したコンピュータ装置においては、アプリケーションプログラムに従って実行される命令コードのうち、実行を制限されている命令コードについては、その命令コードを実行することにより該コンピュータ装置に記憶されているデータが操作される場合には、その命令コードは実行されない。

### 【0014】

#### 【発明の実施の形態】

以下、図面を参照しつつ本発明の実施形態について説明する。

### 【0015】

#### [A. 構成]

##### (1: 通信システムの構成)

図1は、本実施形態に係る端末装置10を有する通信システムの全体構成の一例を示す図である。図1に示されるコンテンツサーバ40は、一般的なコンピュータ装置と同一の構成を有するものであり、インターネット30に接続されている。このコンテンツサーバ40は、端末装置10へ提供するためのアプリケーションプログラム（以下、「APP」と称する）を記憶している。このAPPは、オブジェクト指向のプログラム言語の1つであるJava（登録商標）で記述さ

たものであり、後述する J a v a 実行環境で解釈および実行可能な J a v a バイトコードで構成されている。以下では、このような A P P を「J a v a A P P」と称する。この J a v a A P P は、インターネット 30 を介して端末装置 10 へ提供される非ネイティブ A P P である。

#### 【0016】

移動パケット通信網 20 は、当該移動パケット通信網 20 に収容される端末装置 10 に対して、パケット通信サービスを提供するためのものである。この移動パケット通信網 20 は、基地局 21 とゲートウェイ（以下、「GW」と称する）装置 22 とを有している。基地局 21 は、移動パケット通信網 20 のサービスエリア内に多数設置されている。この基地局 21 は、一定の広さ（例えば、当該基地局 21 を中心とする半径 500 メートルの範囲）を有する無線セルを形成し、この無線セルに在圏する端末装置 10 と無線通信を行うためのものである。GW 装置 22 は、移動パケット通信網 20 における通信プロトコルとインターネット 30 における通信プロトコルとを相互変換し、移動パケット通信網 20 とインターネット 30 との間の通信を仲介するためのものである。

#### 【0017】

端末装置 10 は、J a v a 実行環境を備えた携帯電話機である。この端末装置 10 には、図 2 に示される電話帳テーブルや図 3 に示される着信履歴テーブルなどの端末装置 10 を利用するユーザの個人情報が格納されている。図 2 に示されるように、電話帳テーブルには、このユーザと通話する通信先を一意に特定するための識別子（例えば、通信相手の氏名や名称：以下、「通信先識別子」と称する）に対応付けて、その通信先の電話番号が格納されている。以下では、互いに対応付けられている通信先識別子と電話番号との組を「電話帳データ」と称する。また、図 3 に示されるように、着信履歴テーブルには、この端末装置 10 に対して発信を行った通信先の電話番号（以下、「着信電話番号」と称する）が着信した時刻の順に格納されている。なお、本実施形態では、セキュリティを保護すべきユーザの個人情報の一例として、電話帳テーブルや着信履歴テーブルに格納されているデータについて説明するが、ユーザ自身の電話番号や、このユーザの銀行口座番号およびクレジット番号などであっても良いことは勿論である。

**【0018】**

また、端末装置10は、移動パケット通信網20とインターネット30とを介してコンテンツサーバ40からJavaAPPをダウンロードし、このJavaAPPを上記Java実行環境を用いて実行することができる。本実施形態においては、このJavaAPPは、図4に示されるフローチャートに示される着信通知処理を端末装置10に実行させるものであるとする。具体的には、このJavaAPPを実行中の端末装置10は、図5に示される画面を表示し、この画面の領域520にユーザの所望に応じた画像を表示するとともに、通話着信を待ち受けている。そして、通話着信があった場合に、上記着信履歴テーブルから最新の着信電話番号を取得するとともに、この着信電話番号に対応する電話帳データを上記電話帳テーブル（図2参照）から取得し、その電話帳データを領域510（図5参照）へ表示することにより、通話着信をユーザに報知する。

**【0019】**

（2：端末装置10の構成）

次に、端末装置10のハードウェア構成を、図6を参照しつつ説明する。図6に示されるように、端末装置10は、制御部610と、表示部620と、操作部630と、無線通信部640と、記憶部650と、これら各構成要素間のデータ授受を仲介するバス660とを有している。

**【0020】**

制御部610は、例えばCPU（Central Processing Unit）であり、記憶部650に格納されているソフトウェアを実行することにより端末装置10の各部を制御するものである。表示部620は、例えば液晶ディスプレイとその駆動回路であり、制御部610から引渡された画像データに応じた画像を表示する。操作部630は、数字や文字、操作指示などをユーザに入力させるための複数の操作子を備えており、これらの操作子の操作内容に応じたデータを制御部610へ引渡す。

**【0021】**

無線通信部640は、図示せぬアンテナを備えており、端末装置10の在圏する無線セルを形成する基地局21と無線通信するためのものである。この無線通

信部 6 4 0 は、基地局 2 1 から送信されてくるデータを受信し、受信したデータを制御部 6 1 0 へ引渡すとともに、制御部 6 1 0 から引渡されたデータを基地局 2 1 へ送出する。

#### 【 0 0 2 2 】

記憶部 6 5 0 は、揮発性記憶部 6 5 1 と不揮発性記憶部 6 5 2 とを有している。揮発性記憶部 6 5 1 は、例えば R A M (Random Access Memory) であり、ソフトウェアを実行中の制御部 6 1 0 によりワークエリアとして使用される。この揮発性記憶部 6 5 1 には、J a v a A P P の実行過程において、図 7 に示されるデータ管理テーブル 6 5 1 a が書き込まれる。このデータ管理テーブル 6 5 1 a には、J a v a A P P の実行過程で生成されたオブジェクトを一意に特定するデータ（以下、「参照データ」と称する）に対応付けて、“0”または“1”のいずれか一の値を有する保護フラグが格納される。本実施形態においては、「参照データ」として、揮発性記憶部 6 5 1 内でのオブジェクトの格納位置を示すアドレスを用いるものとする。また、保護フラグは、上記オブジェクトに内包されているデータがセキュリティの保護を要するデータであるか否かを示すものである。本実施形態では、値が“0”である保護フラグを対応付けられているオブジェクトには、セキュリティを保護する必要のないデータが内包されており、逆に、値が“1”である保護フラグを対応付けられているオブジェクトには、セキュリティを保護する必要の有るデータが内包されているものとする。

#### 【 0 0 2 3 】

不揮発性記憶部 6 5 2 は、例えば E E P R O M (Electrically Erasable Programmable Read Only Memory) であり、端末装置 1 0 を利用するユーザの有するデータ毎に上記保護フラグを予め対応付けて格納している。例えば、電話帳テーブル（図 2 参照）や着信履歴テーブル（図 3 参照）などの個人情報には、セキュリティの保護を要することを示す保護フラグが対応付けられており、ユーザの自作画像データなどの個人情報以外のデータには、セキュリティの保護を要さないことを示す保護フラグが対応づけられている。なお、不揮発性記憶部 6 5 2 に格納されている全てのデータについてセキュリティを保護する場合には、上記保護フラグを対応づけておく必要はない。

## 【0024】

加えて、不揮発性記憶部 652 には、図 8 に示すコマンド管理テーブル 652 a を格納している。このコマンド管理テーブル 652 a については後に詳細に説明する。また、この不揮発性記憶部 652 には、J a v a 実行環境を構築するためのソフトウェアや OS を実現するための OS ソフトウェアやネイティブ A P P などが格納されている。このネイティブ A P P の一例としては、電話帳テーブルに格納されている電話帳データをユーザに閲覧させたり更新させたりするための電話帳管理 A P P が挙げられる。

## 【0025】

また、詳細な図示は省略するが、上記不揮発性記憶部 652 には、コンテンツサーバ 40 からダウンロードした J a v a A P P を格納するための記憶領域が J a v a A P P 毎に設けられている。この記憶領域には、上記 J a v a A P P の J A R (Java ARchive) が格納される。J A R ファイルとは、J a v a A P P の本体プログラム (J a v a バイトコードで記述されたプログラム) と、このプログラムを実行する際に使用される画像データを格納した画像ファイルや音声データを格納した音声ファイルなどを 1 つにまとめたファイルである。

## 【0026】

## (3: J a v a 実行環境)

次に、J a v a 実行環境を構築するために端末装置 10 に組み込まれているソフトウェアについて図 9 を参照しつつ説明する。図 9 は、端末装置 10 における J a v a 実行環境を説明するための図である。この図に示されるように、端末装置 10 には、J 2 M E (Java 2 platform Micro Edition) に準拠した J a v a 実行環境を実現するためのソフトウェアが組み込まれている。ここで、J 2 M E とは、小型電子器機向けに定められた J a v a 実行環境の規格である。図 9 に示されるように、上記 J 2 M E を実現するためのソフトウェアには、K V M と、C L D C (Connected Limited Device Configuration) クラスライブラリと、オリジナル J a v a 拡張プロファイルと、J A M (Java Application Manager) とが含まれている。なお、詳細な図示は省略したが、端末装置 10 は、上述した C L D C クラスライブラリやオリジナル J a v a 拡張プロファイルの他に、メーカー独



自拡張ライブラリを有している。このメーカー独自拡張ライブラリは、端末装置 10 の製造者がそれぞれ独自の機能を提供するためのクラスライブラリである。また、本実施形態では、J2ME に準拠した J a v a 実行環境を有する端末装置 10 に本発明を適用する場合について説明するが、J2SE (Java2 Standard Edition) や J2EE (Java2 Enterprise Edition) に準拠した J a v a 実行環境を有する端末装置に本発明を適用するとしても勿論良い。J2SE とは、P C 向けに定められた J a v a 実行環境の規格であり、J2EE とは、例えばコンテンツサーバ 40 のようなサーバ装置向けに定められた J a v a 実行環境の規格である。

#### 【0027】

まず、CLDC クラスライブラリとオリジナル J a v a 拡張プロファイルについて説明する。CLDC クラスライブラリは、携帯電話機や P D A (Personal Digital Assistance) などの小型電子器機向けの汎用的な機能を提供するためのクラスライブラリである。オリジナル J a v a 拡張プロファイルは、CLDC クラスライブラリを基礎として本実施形態に係る端末装置 10 に特化した機能を提供するためのクラスライブラリである。このオリジナル J a v a 拡張プロファイルには、例えば、画面表示 A P I (Application Program Interface)、イベント取得 A P I、ネットワーキング A P I、スクラッチパッド A P I、X - S t r i n g 生成 A P I などが含まれている。J a v a A P P を実行中の制御部 610 は、その J a v a A P P を構成する J a v a バイトコードに従って、これら A P I を呼出すことにより、これら A P I の提供する機能を利用することができる。なお、本明細書および図面においては「A P I」はクラス（プログラム）と同義である。

#### 【0028】

画面表示 A P I とは、表示部 620 への画像の表示をサポートするための A P I である。イベント取得 A P I とは、通話着信や操作部 630 への操作指示の入力などのイベントの発生を J a v a A P P を実行中の制御部 610 に通知することをサポートする A P I である。ネットワーキング A P I とは、U R L (Uniform Resource Locator) により指定されたネットワークリソース（例えば、コンテ

ンツサーバ40)へアクセスするためのAPIである。スクラッチパッドAPIとは、スクラッチパッドに対する書き込みや読み出しをサポートするためのAPIである。なお、スクラッチパッドとは、詳細な図示は省略したが、不揮発性記憶部652内にJavaAPP毎に設けられた記憶領域であり、そのJavaAPPの実行に応じて発生するデータが格納される。

#### 【0029】

X-String生成APIは、不揮発性記憶部652に格納されているデータをJavaAPPを実行中の制御部610に利用させるためのAPIである。本実施形態に係るX-String生成APIは、電話帳テーブルに格納されている電話帳データをJavaAPPを実行中の制御部610に利用させるためのAPIであるとする。より詳細に説明すると、このX-String生成APIを呼出すことにより、最新の着信電話番号に対応した電話帳データを内包したX-Stringオブジェクトが生成され、揮発性記憶部651へ格納されるものとする。加えて、このX-Stringオブジェクトの参照データに対応付けて、このX-Stringオブジェクトに内包されている電話帳データに対応付けられている保護フラグ(すなわち、“1”)がデータ管理テーブル651a(図7参照)へ格納されるものとする。ここで、X-Stringオブジェクトとは、文字列データを格納する一般的なStringオブジェクトに内包されているメソッドのうち、比較メソッドやデータ長通知メソッドを削除したものである。比較メソッドとは、引渡された文字列データと、Stringオブジェクトに内包している文字列データとを比較しその比較結果を呼出し元へ通知するメソッドである。またデータ長通知メソッドとは、Stringオブジェクトに内包されている文字列データのデータ長(例えば、文字数)を呼出し元へ通知するメソッドである。X-Stringオブジェクトがこれらのメソッドを有していない理由は、これらのメソッドが呼出されることにより、このX-Stringオブジェクトに内包されている文字列データの内容を推定されてしまう虞があるからである。なお、本実施形態においては、X-Stringオブジェクトを用いて文字列データのセキュリティを確保する場合について説明したが、本発明の適用対象は文字列データに限定されるものではない。例えば整数型のデータや浮動小数

点型のデータであっても良いことは勿論である。

### 【0030】

そして、上記X-String生成APIを呼出すことにより、最新の着信電話番号データを内包したX-Stringオブジェクトの参照データが制御部610へ引渡される。以降、制御部610は、例えば、この参照データを引数として上記画面表示APIを呼出すことにより、この参照データで示されるX-Stringオブジェクトに内包されている電話帳データを表示部620に表示させることができる。なお、本実施形態においては、X-Stringオブジェクトに最新の着信電話番号に対応する電話帳データを内包させる場合について説明したが、係る電話帳データの一部（例えば、この電話帳データに内包されている電話番号のみや、通信先識別子のみ）を内包させるとしても勿論良い。これらのデータについても、ユーザの個人情報であることには変わらないからである。

### 【0031】

ここで、図8に戻って、コマンド管理テーブル652aについて説明する。このコマンド管理テーブル652aには、上述した各種APIのうち、ネットワークAPIを特定する識別子（例えば、ネットワークAPIの名称：以下、「API識別子」と称する）とスクラッチパッドAPIのAPI識別子とが格納されている。上述したように、JavaAPPを実行中の制御部610は、ネットワークAPIを呼出すことにより、データをCPへ送信することができる。また、制御部610は、スクラッチパッドAPIを呼出すことにより、スクラッチパッドへデータを書き込んだり、スクラッチパッドに格納されているデータを自由に操作することができる。つまり、これらのAPIは、操作対象のデータを端末装置10の外部へ漏洩させてしまう虞があるAPIである。このように、コマンド管理テーブル652aには、セキュリティの保護を要するデータの操作に不適切なAPI、すなわち、個人情報などの重要なデータのセキュリティを保護するために本端末装置10において実行を制限する必要のあるAPIを特定するAPI識別子が格納されている。なお、コマンド管理テーブル652aに格納させておくAPI識別子は、ネットワークAPIやスクラッチパッドAPIのAPI識別子に限定されるものではない。例えば、キャスト処理を行うAP

I（以下、「キャストAPI」と称する）のAPI識別子であっても良い。キャスト処理とは、あるオブジェクトを他の型のオブジェクトへ変換するAPIである。このようなキャスト処理が行われると、X-StringオブジェクトをStringオブジェクトへ変換することが可能になり、X-Stringオブジェクトに内包させていた電話帳データのセキュリティを確保できなくなる虞があるからである。

#### 【0032】

KVMは、JVMの1種であり、携帯電話機やPDA等の小型電子機器用に設計されている。JVMとは、JavaAPPを構成しているJavaバイトコードを制御部610が解釈可能な命令コード（例えば、制御部610のマシン語コード）に変換し、制御部610に実行させるためのものである。このKVMは、JavaAPPを構成しているJavaバイトコードを解釈し実行する際に、本発明に特有な態様でJavaバイトコードの解釈および実行を行う。

#### 【0033】

具体的には、KVMは、実行対象のJavaバイトコードが本端末装置10において実行を制限されているAPIを呼出す旨のJavaバイトコードであるか否かを上記コマンド管理テーブル652a（図8参照）の格納内容に基づいて判定する。そして、実行を制限されているAPIを呼出す旨のJavaバイトコードであると判定した場合には、KVMは、そのAPIにより操作されるデータがセキュリティを保護する必要のあるデータであるか否かを上記データ管理テーブル651a（図7参照）の格納内容に基づいて判定し、セキュリティを保護する必要のあるデータであると判定した場合には、そのJavaバイトコードの解釈実行を行わない。本実施形態に係る端末装置10は、このようにして、セキュリティを保護すべきデータが端末装置10の外部へ漏洩することを防止し、そのデータのセキュリティを確保している。

#### 【0034】

図9に戻って、JAMは、OSによる制御の下で、端末装置10に記憶されているJavaAPPの管理を行うためのソフトウェアである。具体的には、制御部610は、JavaAPPの管理を行うために、JAMに従いJavaAPP

のインストールや、削除を行う機能、不揮発性記憶部 652 に格納されている J a v a A P P の名称をリスト表示する機能、J a v a A P P の実行管理を行う機能を営む。

### 【0035】

J a v a A P P の実行管理を行う機能とは、J a v a A P P の実行の開始および終了を行う機能である。より詳細に説明すると、ユーザに J a v a A P P の実行を指示されると、まず、制御部 610 は J A M に従ってその J a v a A P P を実行するためのワークエリアを揮発性記憶部 651 内に確保する。このワークエリアには、ユーザに実行を指示された J a v a A P P を構成する J a v a バイトコードが展開されたり、この J a v a A P P を実行中にユーザにより入力されたデータが格納される。次に、制御部 610 は、その J a v a A P P を構成している J a v a バイトコードを揮発性記憶部 651 内に確保したワークエリアへ展開し、その J a v a バイトコードを K V M に従って解釈し実行する。そして、ユーザに J a v a A P P の終了を指示されると制御部 610 は、K V M による J a v a バイトコードの解釈および実行を終了するとともに、その J a v a A P P を実行するために揮発性記憶部 651 内に確保したワークエリアを開放し、その J a v a A P P の実行を終了する。

### 【0036】

#### [B. 動作]

次に、本実施形態の動作について説明する。以下では、本実施形態に係る端末装置の特徴を顕著に示す動作について説明する。

### 【0037】

#### (動作例 1：J a v a A P P 実行動作)

ユーザにより J a v a A P P の実行を指示されると、制御部 610 は J A M にしたがってこの J a v a A P P を構成する J a v a バイトコードを揮発性記憶部 651 へ展開する。そして、制御部 610 は、K V M にしたがってこの J a v a バイトコードを解釈および実行することにより、その J a v a A P P を実行する。例えば、制御部 610 は、図 4 に示される着信通知処理を実現する J a v a A P P を実行する場合には、ステップ S A 1 ～ステップ S A 5 の各ステップにおい

て、そのステップを実現する J a v a バイトコードを K V M にしたがって解釈し実行する。以下では、まず、ステップ S A 1 ～ステップ S A 5（図 4 参照）の各ステップにおいて、制御部 6 1 0 が K V M にしたがって実行する J a v a バイトコード解釈・実行動作について図 1 0 を参照しつつ説明する。

#### 【0038】

図 1 0 は、制御部 6 1 0 が K V M にしたがって実行する J a v a A P P 解釈・実行動作の流れを示すフローチャートである。図 1 0 に示されるように、制御部 6 1 0 は、まず、実行対象の J a v a バイトコードが実行を制限されている A P I を呼出す旨の J a v a バイトコードであるか否かをコマンド管理テーブル 6 5 2 a（図 8 参照）の格納内容に基づいて判定する（ステップ S B 1）。具体的には、制御部 6 1 0 は、その J a v a バイトコードを解釈し実行することにより呼出される A P I の A P I 識別子がコマンド管理テーブル 6 5 2 a に格納されている場合には、実行を制限されている A P I を呼出す旨の J a v a バイトコードであると判定し、逆に、その A P I 識別子がコマンド管理テーブル 6 5 2 a に格納されていない場合には、実行を制限されている A P I を呼出す旨の J a v a バイトコードではないと判定する。

#### 【0039】

ステップ S B 1 の判定結果が “N o” である場合には、制御部 6 1 0 は、実行対象の J a v a バイトコードを解釈し命令コードへ変換する（ステップ S B 3）。逆に、ステップ S B 1 の判定結果が “Y e s” である場合には、制御部 6 1 0 は、実行対象の J a v a バイトコードで呼出されている A P I を用いてアクセスしようとしているデータが、セキュリティの保護を要するデータであるか否かをデータ管理テーブル 6 5 1 a（図 7 参照）の格納内容に基づいて判定する（ステップ S B 2）。具体的には、制御部 6 1 0 は、そのデータを示す参照データに、セキュリティの保護を要する旨の保護フラグ（すなわち “1”）が対応づけられている場合には、セキュリティの保護を要するデータであると判定し、逆に、セキュリティの保護を要さない旨の保護フラグ（すなわち “0”）が対応づけられている場合には、セキュリティの保護を要さないデータであると判定する。

#### 【0040】

ステップ S B 2 の判定結果が “N o” である場合には、制御部 6 1 0 は上述したステップ S B 3 を行い、ステップ S B 3 にて得られた命令コードを実行する（ステップ S B 4）。逆に、ステップ S B 2 の判定結果が “Y e s” である場合には、制御部 6 1 0 は、例外処理を行う（ステップ S B 5）。この例外処理の一例としては、例えば、この J a v a A P P は不正な動作を行う虞がある旨の通知をユーザに報知することなどが挙げられる。なお、本実施形態においては、実行を制限されている A P I を呼出す旨の J a v a バイトコードについては、その A P I により操作されるデータがセキュリティの保護を要するデータである場合に、その J a v a バイトコードの解釈および実行を行わないようにする場合について説明した。しかしながら、係る J a v a バイトコードの解釈および実行を行い、その実行過程で上記セキュリティの保護を要するデータへのアクセスが発生した時点で上記例外処理を行うとしても勿論良い。

#### 【 0 0 4 1 】

本動作例においては、図 4 に示されるように、この J a v a A P P には、実行を制限されている A P I を呼出す旨の J a v a バイトコードは内包されていないので、ステップ S A 1 ～ステップ S A 5 の各ステップで上記ステップ S B 3 およびステップ S B 4 が実行され、これら各ステップを実現する J a v a バイトコードが実行される。

#### 【 0 0 4 2 】

図 4 に戻って、J a v a A P P に内包されている J a v a バイトコードを制御部 6 1 0 が実行することにより実現される着信通知処理について説明する。図 4 に示されるように、制御部 6 1 0 は、まず、画面表示 A P I を呼出し、図 5 に示される画面を表示部 6 2 0 に表示させ（ステップ S A 1）、イベント取得 A P I を呼出し、通話着信があったか否かを判定する（ステップ S A 2）。そして、制御部 6 1 0 は、ステップ S A 2 の判定結果が “N o” である場合には、後述するステップ S A 5 の処理を実行し、逆に、ステップ S A 2 の判定結果が “Y e s” である場合には X - S t r i n g 生成 A P I を呼出し、その通話着信についての電話帳データを内包した X - S t r i n g オブジェクトの参照データを取得する（ステップ S A 3）。

## 【0043】

ここで、ステップSA3にて呼出されるX-String生成APIを実行中の制御部610により実行される電話帳データ取得処理について図11を参照しつつ説明する。図11は、電話帳データ取得処理の流れを示すフローチャートである。図11に示されるように、制御部610は、まず、着信履歴テーブル（図3参照）から最新の着信電話番号を取得し（ステップSC1）、取得した着信電話番号と同一の電話番号を内包した電話帳データを電話帳テーブル（図2参照）から取得する（ステップSC2）。

## 【0044】

次に、制御部610は、ステップSC2にて取得した電話帳データを内包したX-Stringオブジェクトを生成し（ステップSC3）、このX-Stringオブジェクトの参照データと、このX-Stringオブジェクトに内包されている電話帳データの保護フラグとを対応づけて、データ管理テーブル651aへ格納する（ステップSC4）。

## 【0045】

そして、制御部610は、ステップSC3にて生成したX-Stringオブジェクトの参照データと呼出し元のJavaAPPへ引渡し、X-String生成APIの実行を終了する（ステップSC5）。

## 【0046】

図4に戻って、ステップSA3にてX-String生成APIを呼出すことにより、通話着信についての電話帳データを内包したX-Stringオブジェクトの参照データを取得した制御部610は、この参照データを表示部620へ引渡し、この参照データで示されるX-Stringオブジェクトに内包されている電話帳データを図5に示す画面の領域510へ表示させる（ステップSA4）。

## 【0047】

（動作例2：実行を制限されているAPIを呼出すJavaAPPを実行する場合の動作）

次いで、図12に示す着信通知処理を実現するJavaAPPを制御部610



が実行する場合について説明する。図12に示される着信通知処理が図4に示される着信通知処理と異なっている点は、ステップSA6を有する点のみである。このステップSA6は、ステップSA3にて取得した通信先識別子をネットワークAPIを用いてJavaAPPの提供元のコンテンツサーバ40へ送信するステップである。つまり、図12に示される着信通知処理を実現するJavaAPPは、通話着信があった場合に、その通話着信についての電話帳データを盗み出しコンテンツサーバ40へ送信するものであり、悪意のあるCPにより提供されたJavaAPPである。なお、このようなJavaAPPを実行する場合であっても、ステップSA6以外のステップについては、図4に示される着信通知処理と同一の処理が行われる。このため、これらのステップにおける制御部610の動作については説明を省略し、ステップSA6を実現するJavaバイトコードをKVMにしたがって解釈し実行する際の制御部610の動作についてのみ、図12を参照しつつ説明する。

#### 【0048】

ステップSA6（図12参照）を実現するJavaバイトコードは、ネットワークAPIを呼出す旨のJavaバイトコードであるから、上述したステップSB1における判定結果は“Y e s”となり（図8および図10参照）、制御部610は上述したステップSB2の処理を行う。

#### 【0049】

ネットワークAPIを用いてコンテンツサーバ40へ送信されるデータは、電話帳データであるから、上述したステップSB2における判定結果は“Y e s”となり、制御部610は上述した例外処理を行う（ステップSB5）。その結果、ステップSA6（図12参照）を実現するJavaバイトコードが実行されることはなく、電話帳データを盗み出されることが防止される。

#### 【0050】

以上説明したように、非ネイティブAPPの実行過程で端末装置10に記憶されている重要なデータを利用することが可能になるとともに、この重要なデータのセキュリティを確保することが可能になる。

#### 【0051】

## 〔C．変形例〕

以上、本発明の実施形態について説明したが、本発明は係る実施形態に限定されるものではなく、その技術思想の範囲内で様々な変形が可能である。なお、変形例としては、例えば、以下のようなものが考えられる。

## 【0052】

（変形例1）上述した実施形態では、非ネイティブAPPの一例として、Java バイトコードで構成されたAPPについて説明したが、非ネイティブAPPを記述するプログラミング言語はJavaに限定されるものではない。他のプログラミング言語（例えば、C++やC言語）であっても良い。一般に、これらのプログラミング言語で記述されたAPPは、その提供時点で命令コードに変換されている。このような場合には、上述したKVMに替えて、図10に示されるフローチャートに従った動作を行うプログラムを端末装置10に記憶させておく必要がある。なお、このようにして提供されるAPPは既に命令コードで構成されているため、ステップSB3の処理を行う必要はない。

## 【0053】

（変形例2）上述した実施形態では、Java 実行環境を有する携帯電話機に本発明を提供する場合について説明した。一般に携帯電話機には、電話帳テーブルや着信履歴テーブルなどの個人情報記憶されているため、本発明を適用した場合に最も顕著な効果が得られる。しかしながら、本発明の適用対象は係る携帯電話機に限定されるものではない。例えば、Java 実行環境を備えたPDAやPHS（Personal Handyphone System：登録商標）端末であっても良く、Java 実行環境を有するPCであって、図13に示されるように、GW装置50を介してインターネット30に接続されたLAN60を構成するもPC70A～70Cであっても良い。要は、Java 実行環境を備え、Java APPを実行する機能を有するコンピュータ装置であれば、いずれであっても良い。

## 【0054】

（変形例3）上述した実施形態では、非ネイティブAPPの一例として、インターネットを介してダウンロードされたJava APPについて説明した。しかしながら、端末装置10にインストールされる非ネイティブAPPは、ダウンロ

ードされた J a v a A P P に限定されるものではなく、例えば C D - R O M などのコンピュータ装置読み取り可能な記録媒体に記録されて配布される J a v a A P P であっても良い。

#### 【0055】

なお、インターネットを介して提供される A P P や、記録媒体に記録されて配布される A P P であっても、例えば、移動パケット通信網 20 を運営する通信事業者や C A (Certificate Authority) のような公正な第三者機関により、その内容が審査され、一定の動作基準を満たしていると認定された A P P (以下、「トラステッド A P P 」という) であれば、ネイティブ A P P と同様にアクセス可能なリソースを制限する必要はない。

#### 【0056】

例えば、トラステッド A P P には、自身がトラステッド A P P であることを示す識別情報を内包させておくとともに、図 14 に示される J a v a バイトコード解釈実行動作を制御部 610 に実行させるとしても良い。図 14 に示される J a v a バイトコード解釈・実行動作が図 10 に示される J a v a バイトコード解釈・実行動作と異なっている点は、上述したステップ S B 1 の前に、ステップ S B 0 を行う点のみである。このステップ S B 0 においては、制御部 610 は実行対象の J a v a A P P がトラステッド A P P であるか否かを判定する。具体的には、制御部 610 は、実行対象の J a v a A P P に上記識別情報が内包されている場合にのみ、その J a v a A P P をトラステッド A P P と判定する。そして、ステップ S B 0 の判定結果が “Y e s ” である場合には、制御部 610 は、無条件に上述したステップ S B 3 を実行し、その J a v a A P P を構成している J a v a バイトコードを解釈し実行する。これは、トラステッド A P P については、ユーザにとって不利益な動作を行わないことが確認されているため、その実行過程でのリソースへのアクセス態様を制限する必要がないからである。

#### 【0057】

(変形例 4) 上述した実施形態では、X - S t r i n g 生成 A P I や K V M など、本発明に係る端末装置に特有な機能を実現するためのソフトウェアを端末装置 10 に予め記憶させておく場合について説明した。しかしながら、コンピュー

タ装置読み取り可能な記録媒体にこれらのソフトウェアを記録しておき、この記録媒体を用いて、これらのソフトウェアを一般的なコンピュータ装置にインストールすることにより、係るコンピュータ装置に端末装置 10 と同一の機能を付与することも可能である。

#### 【0058】

##### 【発明の効果】

本発明によれば、端末装置に記憶されている重要なデータを非ネイティブAPPに利用させることを可能にしつつ、この重要なデータのセキュリティを確保することができるといった効果を奏する。

##### 【図面の簡単な説明】

【図1】 本発明に係る端末装置 10 を有する通信システムの構成例を示す図である。

【図2】 端末装置 10 に記憶されている電話帳テーブルの一例を示す図である。

【図3】 端末装置 10 に記憶されている着信履歴テーブルの一例を示す図である。

【図4】 同端末装置 10 に記憶されているJavaAPPに従って端末装置 10 が行う着信通知処理の流れを示すフローチャートである。

【図5】 同端末装置 10 に表示される画面の画面フォーマットの一例を示す図である。

【図6】 同端末装置 10 の構成の一例を示す図である。

【図7】 同端末装置 10 の揮発性記憶部 651 へ書き込まれるデータ管理テーブルの一例を示す図である。

【図8】 同端末装置 10 の不揮発性記憶部 652 に格納されているコード管理テーブルの一例を示す図である。

【図9】 同端末装置 10 に組み込まれているJava実行環境を説明するための図である。

【図10】 同端末装置 10 の制御部 610 がKVMに従って行うJavaバイトコード解釈実行処理の流れを示す図である。

【図 11】 同端末装置 10 の制御部 610 が X-String 生成 API に従って行う電話帳データ取得処理の流れを示すフローチャートである。

【図 12】 同端末装置 10 に記憶されている Java APP に従って端末装置 10 が行う着信通知処理の流れを示すフローチャートである。

【図 13】 変形例 2 に係る通信システムの構成例を示す図である。

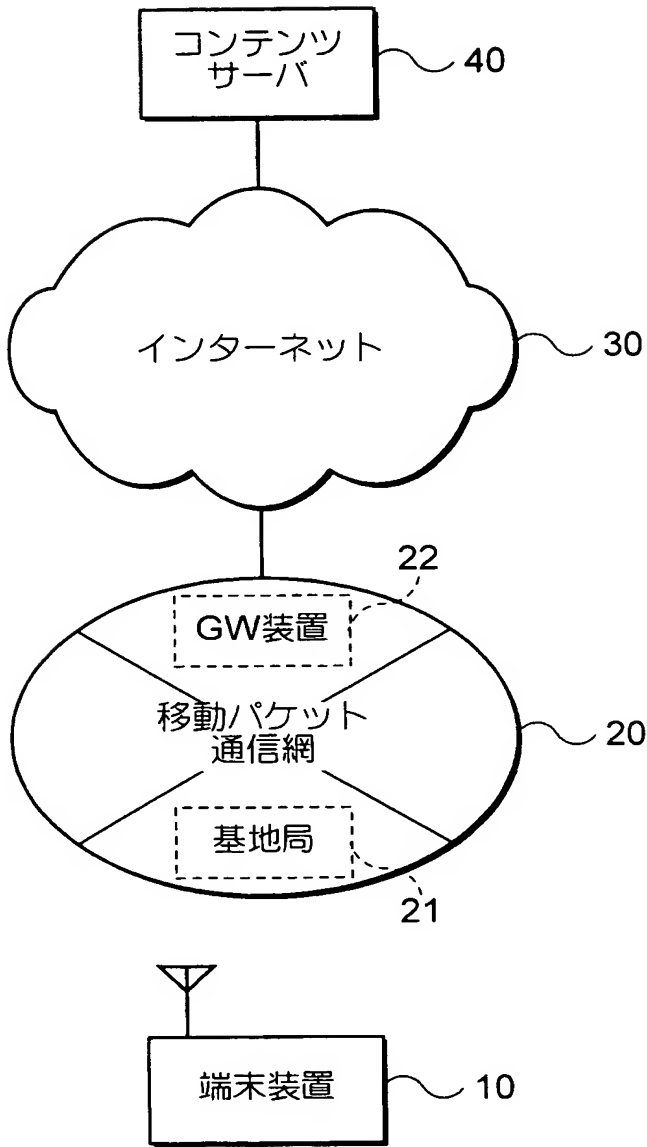
【図 14】 変形例 3 に係る Java バイトコード解釈実行処理の流れを示すフローチャートである。

【符号の説明】

10…端末装置、20…移動パケット通信網、21…基地局、22…ゲートウェイ装置、30…インターネット、40…コンテンツサーバ、610…制御部、620…表示部、630…操作部、640…無線通信部、650…記憶部、651…揮発性記憶部、652…不揮発性記憶部、651a…データ管理テーブル、652a…コマンド管理テーブル、660…バス。

【書類名】 図面

【図 1】



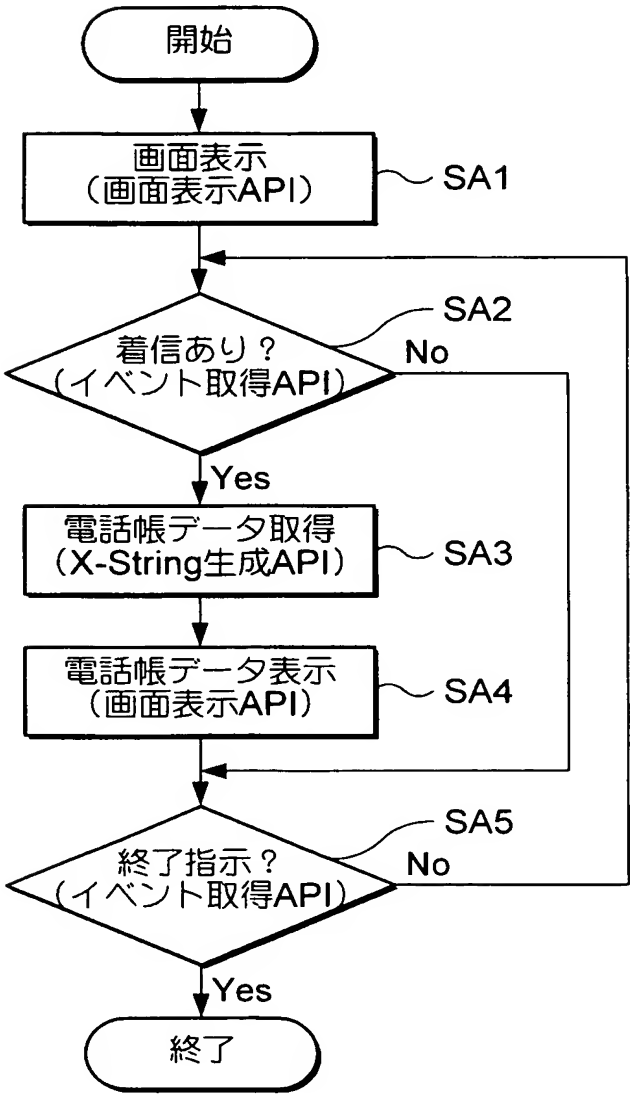
【図 2】

電話番号	通信先識別子
090AAAAAAAAA	AAAA
090BBBBBBBBB	BBBB
090CCCCCCCCC	CCCC

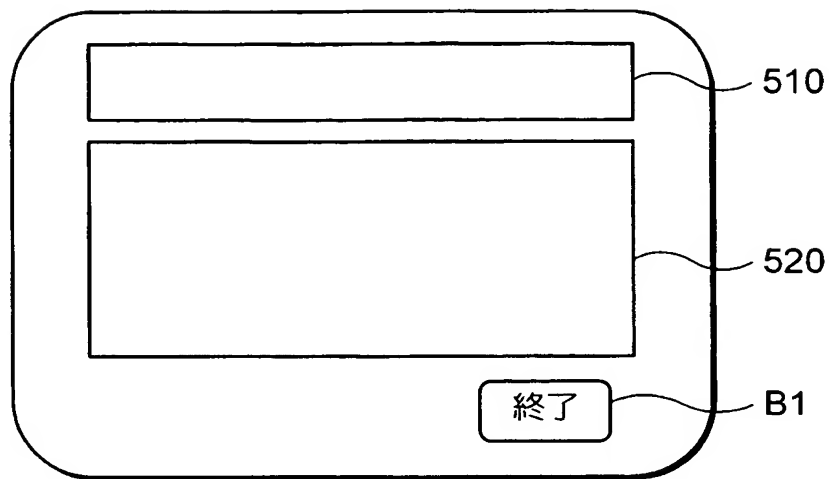
【図 3】

着信電話番号
090XXXXXXXXX
090YYYYYYYYY
090CCCCCCCCC

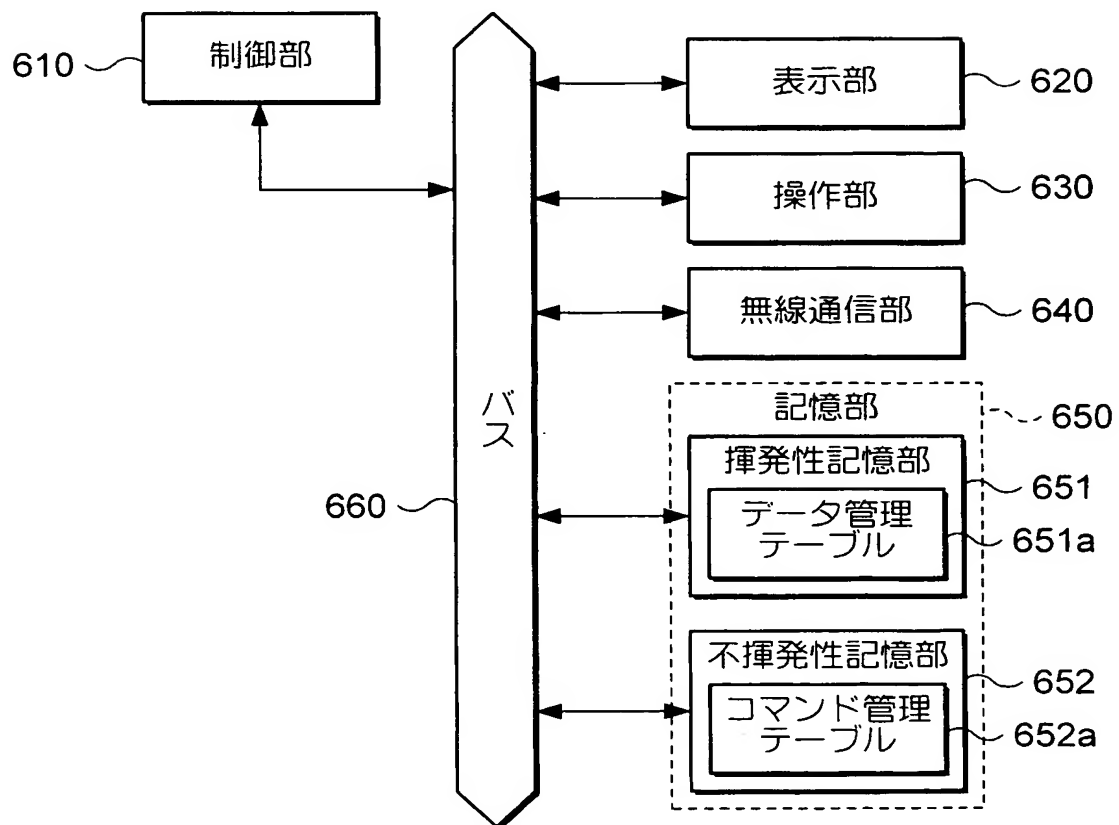
【図 4】



【図 5】



【図 6】





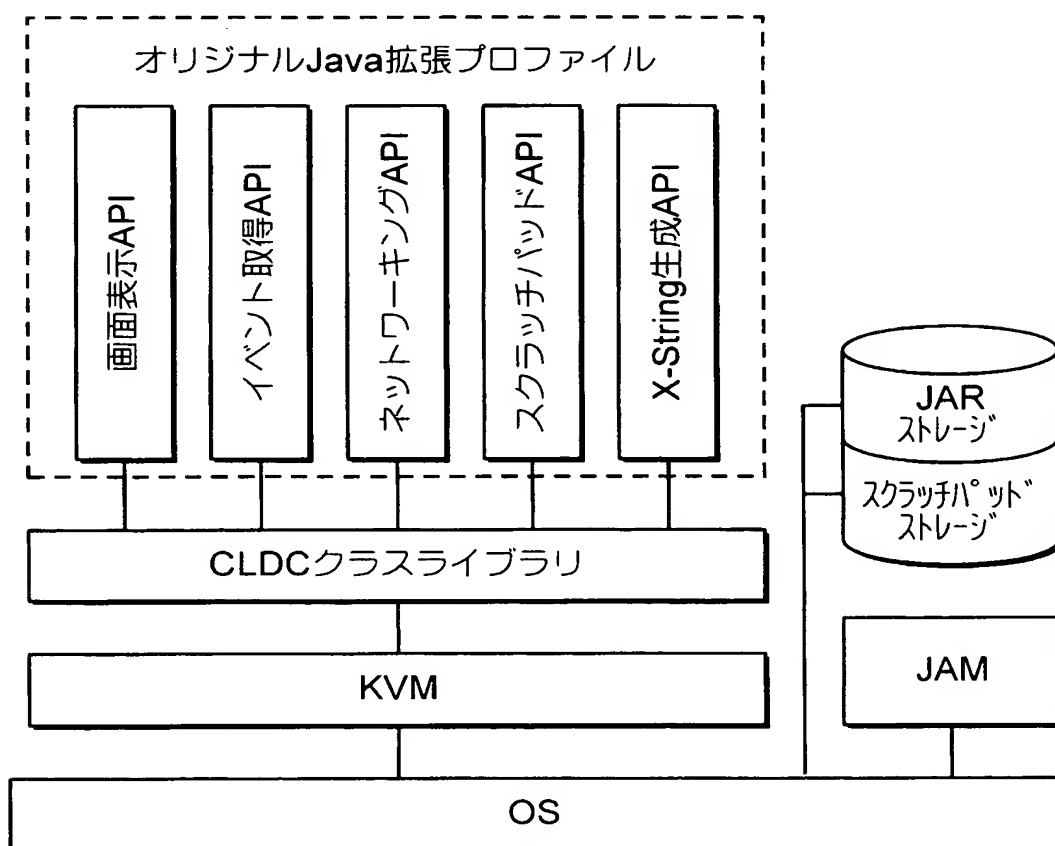
【図7】

参照データ	保護フラグ	651a
0x01(X-Stringのアドレス)	1	

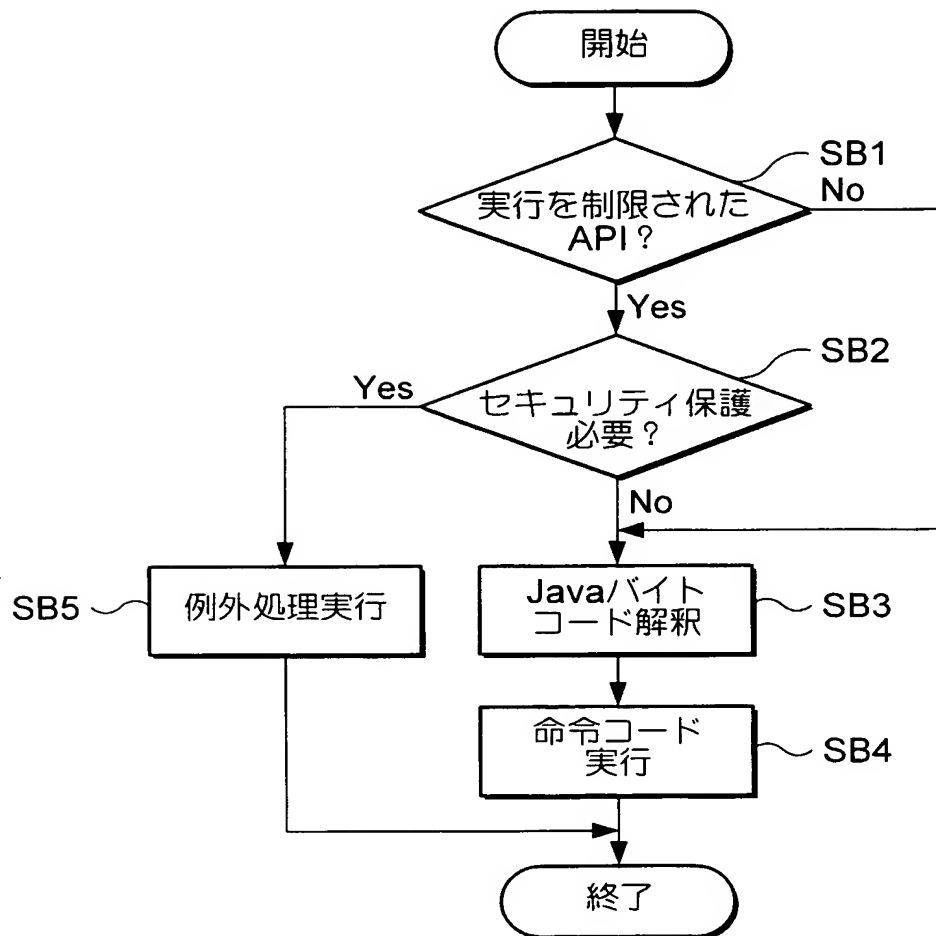
【図8】

API識別子	652a
スクラッチパッドAPI	
ネットワーキングAPI	

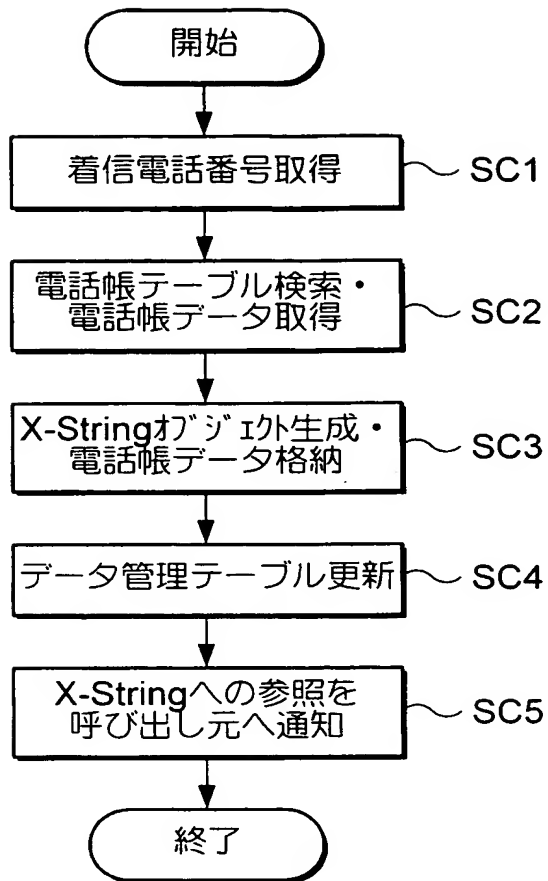
【図9】



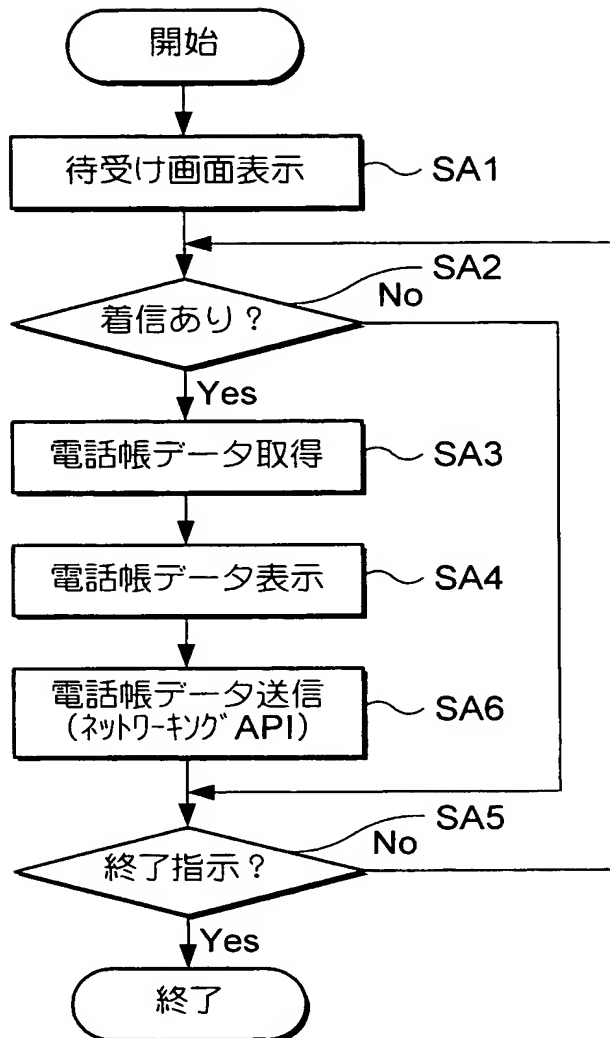
【図 10】



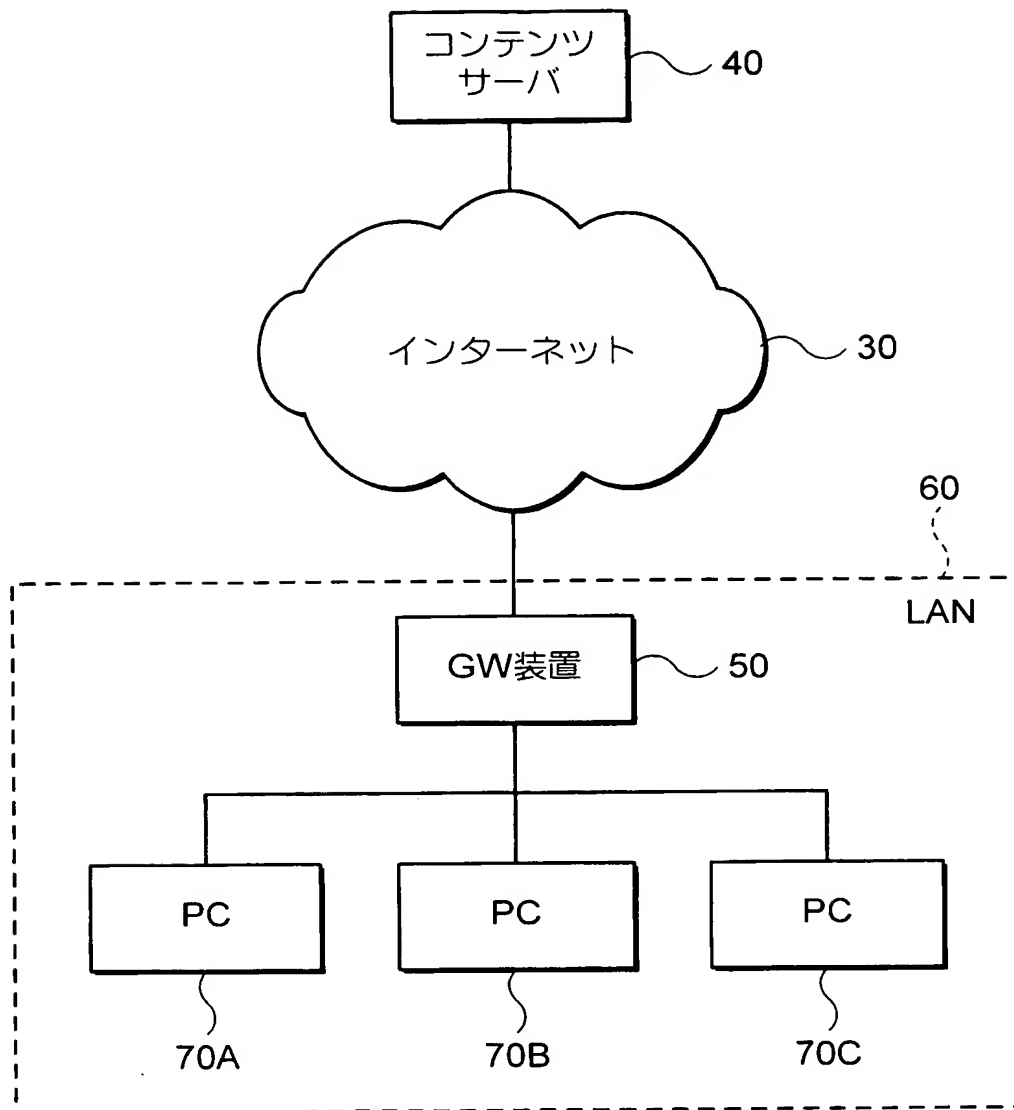
【図 11】



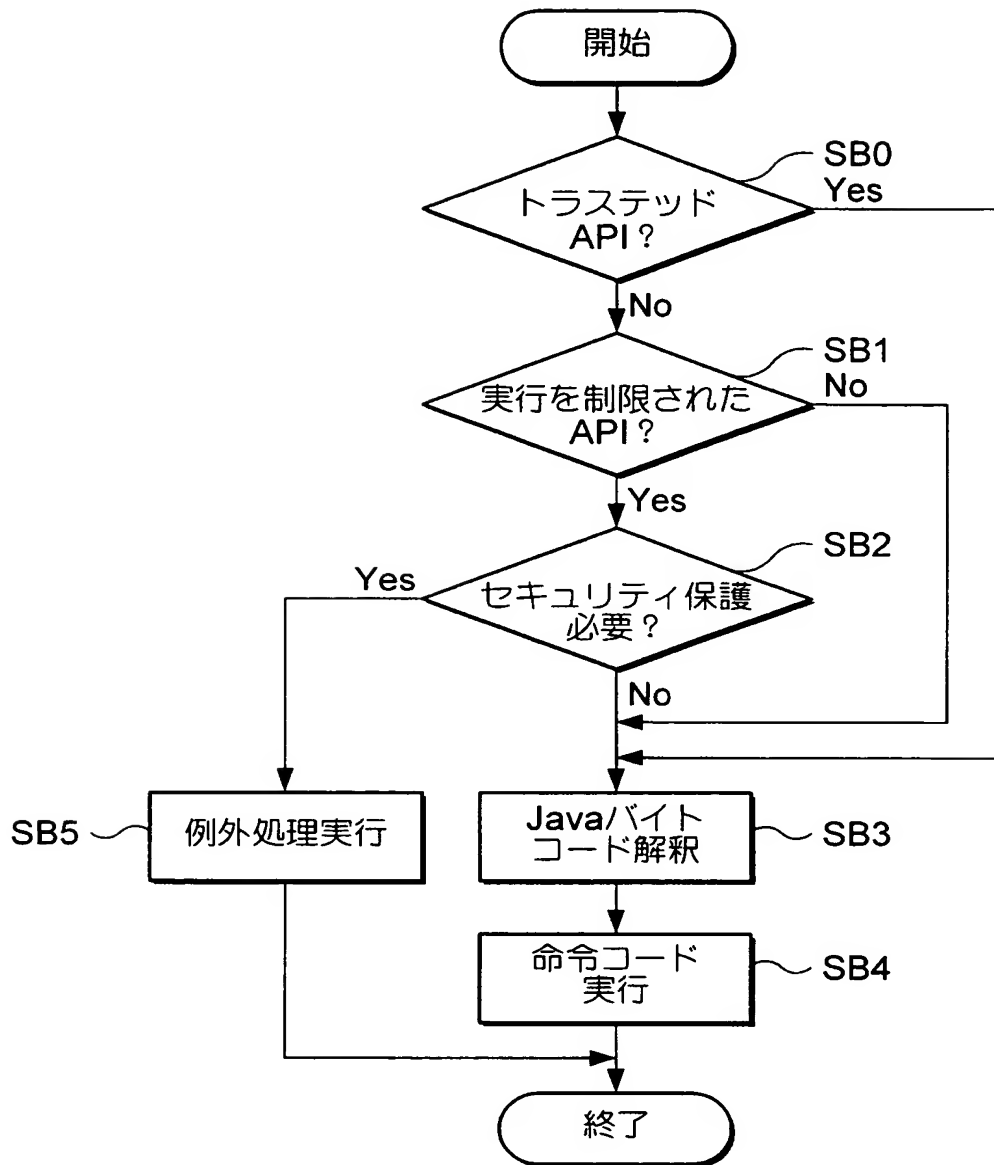
【図 12】



【図 13】



【図 14】



【書類名】 要約書

【要約】

【課題】 端末装置に記憶されている重要なデータを非ネイティブアプリケーションプログラムが利用することを可能にしつつ、この重要なデータのセキュリティを確保する。

【解決手段】 端末装置に、アプリケーションプログラムにしたがって命令コードを実行させる際に、命令コードが本端末装置において実行を制限されている命令コードであるか否かを判定させる。そして、実行を制限されている命令コードであり、かつ、該命令コードを実行することにより本端末装置に記憶されているデータの少なくとも一部分がアクセスされる場合には、該命令コードの実行を禁止する。

【選択図】 図 1 0

特願 2 0 0 3 - 0 9 1 2 9 4

出 願 人 履 歴 情 報

識別番号 [ 3 9 2 0 2 6 6 9 3 ]

1. 変更年月日 2 0 0 0 年 5 月 1 9 日

[変更理由] 名称変更

住所変更

住 所 東京都千代田区永田町二丁目 1 1 番 1 号  
氏 名 株式会社エヌ・ティ・ティ・ドコモ